



plusID™

Tips for IT administrators when configuring a Microsoft® server for logon using the plusID™ biometric device

The **plusID** device is ISO 7816 Part 3 smart card compliant, and as such enumerates itself to a computer exactly like a smart card, allowing for rapid enterprise integration of **plusID** devices across Microsoft® systems that support smart cards.

The following are tips for configuring a Microsoft® environment to support smart cards (i.e., **plusID**):

- If no Certification Authority (CA) exists on your domain, the simplest way to add smart card support is to install Microsoft® Certificate Services in the domain controller.
- The preferred way to install Microsoft Certificate Services is to use the Add/Remove Windows Components option from the Add/Remove Programs control panel applet. Privaris does not recommend installing Certificate Services using the Microsoft Management Console (MMC), as not all required components are installed.
- Certificate Services includes a web-based interface for issuing smart card certificates which is commonly referred to as Web Enrollment. In order to use this feature, Internet Information Services (IIS) must be installed on the same machine as Certificate Services. It is recommended that IIS be installed first so that it may be automatically configured during the installation of Certificate Services.
- If Certificate Services is installed before IIS, IIS will not be automatically configured to enable the Certificate Services web interface. In order to perform this configuration, the following command should be issued at the Command Prompt to create the virtual roots required for Web Enrollment:

```
certutil -vroot
```

- The default installation of Certificate Services does not enable the certificate templates needed for smart card deployment. Before the CA will issue smart card certificates, it must be configured to allow the following certificate templates to be issued:

Enrollment Agent	
Smart Card Login	(for smart card login only)
Smart Card User	(for both smart card login and secure email)

- The Web Enrollment component uses an ActiveX control to issue smart cards. This Microsoft-supplied control is flagged as “dangerous” and is disabled when Internet Explorer (IE) version 7 is used to access the Web Enrollment feature. In order to use IE7, the machine hosting Web

Enrollment pages must be added to the IE7's Trusted Sites list and the Security Level for trusted sites must be set to Low. These settings are accessible through the Security tab of the Internet Options control panel applet.

- During installation of Certificate Services, a self-signed root certificate is generated for the certificate authority. This certificate must be imported into each machine's certificate store within the domain in order for the certificate authority to be recognized. Usually, this is done automatically when machines synchronize with the domain controller however, this does not always happen immediately after installation of Certificate Services. To check if the root certificate has propagated correctly, open each machine's certificate store and look under "Trusted Root Certificate Authorities" for a certificate issued to and issued by the machine hosting Certificate Services. If this is not found, the root certificate can be manually exported from the CA and imported into each machine.
- Additionally, below are useful website links for troubleshooting smart cards for Windows:

<http://support.microsoft.com/kb/308160>

<http://support.microsoft.com/kb/324276>

<http://msdn2.microsoft.com/en-US/library/ms953432.aspx>

<http://technet2.microsoft.com/windowsserver/en/library/88943c7a-8369-4193-a783-765305d1d5ef1033.msp?mfr=true>

<http://technet2.microsoft.com/windowsserver/en/library/6b8b0794-a3d8-4e89-81a3-25a0a84e9d961033.msp?mfr=true>